UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,439	03/02/2004	Ori Eisen	2311.008	3435

7590 05/09/2008

U.P. PETER ENG
WILSON SONSINI GOODRICH AND ROSATI
650 PAGE MILL ROAD
PALO ALTO, CA 94304

EXAMINER	
ZELASKIEWICZ, CHRYSTINA E	
ART UNIT	PAPER NUMBER
4143	

MAIL DATE	DELIVERY MODE
05/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/791,439	EISEN, ORI	
	Examiner	Art Unit	
	Chrystina Zelaskiewicz	4143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *March 7, 2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is in reply to the response filed on 7 March 2008.

2. Claims 19-24 have been added.

3. Claims 1-4, 7, 11-18 have been amended.

4. Claims 1-24 are currently pending and have been examined.

Information Disclosure Statement

5. The Information Disclosure Statement filed on 7 March 2008 has been considered. Initialed copies of the Form 1449 are enclosed herewith.

Drawings

6. In light of Applicant's response, the objection is withdrawn.

Specification

7. Examiner thanks Applicant for deleting references to "the chart" on page 5 of the specification. Examiner notes that one reference still remains on page 5; specifically, the title "DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT AND **THE CHART**." Examiner requests such reference to "the chart" be deleted.

Claim Objections

8. In light of Applicant's amendment of claim 17, which now depends from claim 12, the objection is withdrawn.

Claim Rejections - 35 USC § 112, 2nd paragraph

9. In light of Applicant's amendment of claims 1, 3, 4, 7, 12, 14 and 15 the previous rejections are withdrawn.

10. In light of Applicant's new claims 21-23, please see the rejection below.

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 21-23 are rejected under 35 U.S.C. 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 21-23 use the word *substantially* in their limitations. The word "substantially" is vague and indefinite because it has subjective meaning, and does not further limit nor clarify the subsequent words. For example, claim 21 states *whether they are substantially the same*; this does not indicate whether the parameters are the same or not. Claim 22 states *parameter is substantially constant;* this does not indicate whether the parameters are constant. Claim 23 states *within a substantially constant range;* this does not indicate whether the range is constant or not. For purposes of this examination, the examiner will assume the word "substantially" is omitted from claims 21-23.

Claim Rejections - 35 USC § 101

13. In light of Applicant's amendment of claims 12-18 the rejections are withdrawn.

Response to Arguments

14. The Examiner has pointed out particular references contained in the prior art of record within the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

15. Applicant's arguments have been fully considered, but they are not persuasive. With regard to claims 1 and 5, Applicant argues that "Shinzaki fails to disclose or suggest a delta of time parameter and at least one non-personal identification parameter." Examiner respectfully disagrees. Please see the following passage of Shinzaki that discloses a delta of time parameter (see at least C 4, L 65-67 and C 5, L 1-3: *a* ***time stamp verifying section for comparing the original time stamp****, which has been restored by the decryption section,* ***with the current time****, which has been calculated by the clock function section*). With regard to the one non-personal

identification parameter, this argument is moot for the following reasons: claims 1 and 5 have been rejected on new grounds in light of Applicant's amendment. Please see the rejection below. With regard to claim 12, Applicant argues that "Shinzaki fails to disclose or suggest a computer program for identifying a customer with customer identification data that is based upon both a delta of time parameter AND at least one personal or non-personal identification parameter." Again, Examiner respectfully disagrees. In addition to the passage above that discloses a delta of time parameter, please see the following passages of Shinzaki (see at least column 5, lines 12-15: the **user is identified** as the authorized user of the portable electronic device, as the comparison result by the biometric feature data (at least one personal identification parameter) verifying section and the time stamp verifying section (delta of time parameter)).

16. With regard to claims 2-4, 6-11, 13-18, Applicant made a general argument that these claims are not disclosed in the art. However, Applicant has not given any reasons for this conclusion. Therefore, the rejection stands.

Claim Rejections - 35 USC § 102

17. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

18. Claim 12 is rejected under 35 U.S.C. 102(e) as being anticipated by Shinzaki (US 6,957,339 B2).

Claim 12

Shinzaki, as shown, discloses the following limitations:

- *computer code that receives from an online customer's computer, at least one of either a personal or non-personal identification parameter* (see at least column 3, lines 66-67 and

column 4, lines 1-9: The portable electronic device includes: a biometric feature data register section having pre-stored valid biometric feature data of an authorized user of the portable electronic device; a second transceiving interface for transmitting/receiving data to/from the data processing device; a biometric feature data verifying section for comparing to-be-verified biometric feature data, which is received from an external device via the second transceiving interface, with the valid biometric feature data; and a PIN register section having a pre-stored PIN of the authorized user of the portable electronic device);

- *computer code that captures from a clock of said customer's computer, said customer's computer's local time* (see at least column 4, lines 57-58: a time stamp generating section for generating a time stamp as the date and time)*;*
- *computer code that captures from a clock of a website server, said website server's local time* (see at least column 4, lines 65-66: a clock function section for calculating the current time);
- *computer code that creates and stores a delta of time parameter based upon the difference between said customer's computer's local time and said website server's local time* (see at least column 4, lines 66-67 and column 5, lines 1-3: a time stamp verifying section for comparing the original time stamp… with the current time, which has been calculated by the clock function section); and
- *computer code that identifies said customer with customer identification data that is based upon both said delta of time parameter and at least one of either of said personal or non-personal identification parameter* (see at least column 5, lines 12-15: the user is identified as the authorized user of the portable electronic device, as the comparison result by the biometric feature data verifying section and the time stamp verifying section).

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

21. Claims 1-3, 5-10, 13-16, 18-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shinzaki in view of Ronning et. al. (US 7,165,051 B2).

Claim 1

Shinzaki, as shown, discloses the following limitations:

- *capturing, from a clock of said customer's computer, said customer's computer local time* (see at least column 4, lines 57-58: a time stamp generating section for generating a time stamp as the date and time);
- *capturing, from a clock of a website server, said website server's local time* (see at least column 4, lines 65-66: a clock function section for calculating the current time);
- *creating and storing a delta of time parameter based upon the difference between said customer's computer local time and said website server's local time* (see at least column 4, lines 66-67 and column 5, lines 1-3: a time stamp verifying section for comparing the original time stamp… with the current time, which has been calculated by the clock function section);
- *identifying said customer with said delta of time parameter* (see at least column 5, lines 12-15: the user is identified as the authorized user of the portable electronic device, as the comparison result by the biometric feature data verifying section and the time stamp verifying section).

Shinzaki does not disclose the following limitation, but Ronning, as shown, does:

- *receiving, from a customer's computer, at least one non-personal identification parameter* (see at least column 8, lines 22-23: information may include the following for each order… IP address).
- *identifying said customer with at least one non-personal identification parameter* (see at least column 8, lines 22-23: information may include the following for each order… IP address).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning. Shinzaki discloses capturing a computer's local time, capturing a website server's local time, storing a delta of time parameter, and identifying a customer with this delta of time parameter. Shinzaki does not disclose receiving a non-personal identification parameter or identifying a customer with said non-personal identification parameter. However, Ronning discloses receiving a non-personal identification parameter and identifying a customer with said non-personal identification parameter. Therefore, it would have been obvious to combine Ronning with Shinzaki because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Utilizing a non-personal identification parameter is one measure to help identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

Claim 2

Shinzaki, in view of Ronning, discloses the limitations of claim 1 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *receiving, from said customer's computer, an additional identification parameter comprising personal identification information relating to said transaction* (see at least column 7, lines 55-59: Order form 520 includes a number of sections for receiving the following information for use in submitting an order: name section 521; company name section 522; address section 523; phone section 524; e-mail address section 525; credit card number section 526; and password section 527).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Utilizing a personal identification parameter is one measure to help identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

Claim 3

Shinzaki, in view of Ronning, discloses the limitations of claim 1 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *said at least one non-personal identification parameter is said customer's computer's IP address* (see at least column 8, lines 22-23: information may include the following for each order… IP address).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Utilizing a customer's computer's IP address is one measure to help identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

Claim 5

Shinzaki, in view of Ronning, discloses the limitations of claim 1 as shown above. Furthermore, Shinzaki, as shown, discloses the following limitation:

- *said delta of time parameter is stored as a range of time* (see at least column 4, lines 66-67 and column 5, lines 1-3, 8-10: a time stamp verifying section for comparing the original time stamp… with the current time, which has been calculated by the clock function section… difference between the time stamp and the current time falls within a predetermined range).

Claim 6

Ronning, as shown, discloses the following limitations:

- *creating a first computer identifier in the course of an online transaction comprising the steps of Claim 1* (Shinzaki, in view of Ronning, discloses the limitations of claim 1 as shown above);
- *creating at least a second computer identifier in the course of a second proposed online transaction comprising the steps of Claim 1* (Shinzaki, in view of Ronning, discloses the limitations of claim 1 as shown above);
- *utilizing a matching parameter to compare said first computer identifier with said second computer identifier* (see at least column 9, lines 48-59: The fraud processing involves generating a fraud ranking based upon the user's information in order form 520 and associated information. The associated information may include any information, or a sub-set of that information, having any type of relation to the information submitted with the order. For example, it typically includes information linked with the submitted information as determined by the relational database tables illustrated in FIG. 5C. It may also include a previous fraud ranking or an AVS rating. System 200 may use the submitted information to perform database look ups to obtain associated information for analysis);
- *creating a matching value based on the similarities between said first computer identifier and said second computer identifier* (see at least column 9, lines 65-67 and column 10, line 1: The fraud processing involves comparing the fraud ranking to a particular fraud scale (step 505); for example, a numeric scale with increasing numbers indicating an increasing likelihood of a fraudulent transaction); and
- *classifying said second online transaction as fraudulent, not fraudulent, or requiring further consideration based upon the value of said matching parameter* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order (step 509)… System 200 may perform steps 601 604 in any particular order to generate the cumulative fraud ranking, and may perform fewer steps to generate it or perform more steps based upon additional criteria).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 7

Shinzaki, in view of Ronning, discloses the limitations of claim 6 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *communicating to a website operator an indication, as to whether said second online transaction is fraudulent, not fraudulent, or requires further consideration* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order (step 509)… System 200 may perform steps 601 604 in any particular order to generate the cumulative fraud ranking, and may perform fewer steps to generate it or perform more steps based upon additional criteria).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 8

Shinzaki, in view of Ronning, discloses the limitations of claim 6 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *blocking said second online transaction based upon the value of said matching parameter* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 9

Shinzaki, in view of Ronning, discloses the limitations of claim 6 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *communicating to said customer the status of said second online transaction based upon the value of said matching parameter* (see at least column 7, lines 39-42: System 200 determines if the user is attempting a fraudulent transaction and, if not, it downloads the purchased products to the user's machine using a download page 516; also see at least column 9, lines 34-37: If authorization is not obtained (step 503), system 200 declines the order (step 509) and typically presents a message to the user indicating the denial).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 10

Shinzaki, in view of Ronning, discloses the limitations of claim 6 as shown above. Furthermore, Shinzaki, as shown, discloses the following limitation:

- *said delta of time parameter is stated as a range of time* (see at least column 4, lines 66-67 and column 5, lines 1-3, 8-10: a time stamp verifying section for comparing the original time stamp… with the current time, which has been calculated by the clock function section… difference between the time stamp and the current time falls within a predetermined range).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 13

Shinzaki discloses the limitations of claim 12 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *computer code that receives and stores, from said customer's computer, personal identification information relating to said transaction* (see at least figure 2 as well as column 3, lines 65-67 and column 4, line 1: A log in module 208 receives the request and records certain data associated with the request, such as the user's request, Internet Protocol (TIP) address, date and time, and particular demographic information).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Utilizing personal identification information is one

measure to help identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

Claim 14

Shinzaki discloses the limitations of claim 12 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *computer code that communicates to a website operator an indication as to whether a second online transaction is or is not fraudulent because of the similarity existing between the stored customer identification data and new customer identification data* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order (step 509)… System 200 may perform steps 601 604 in any particular order to generate the cumulative fraud ranking, and may perform fewer steps to generate it or perform more steps based upon additional criteria; also see at least column 12, lines 8-11: system 200 compares particular main information on the same order against known profiles indicating attempted fraudulent transactions (step 712), and it determines if the main information matches the known profiles).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Checking for the similarity between stored customer identification data and new customer identification data can help properly identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

Claim 15

Shinzaki, in view of Ronning, discloses the limitations of claim 14 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *computer code that blocks said second online transaction based upon said indication as to whether a second online transaction is or is not fraudulent* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). If there is an indication that a transaction is fraudulent, then said transaction should be blocked to prevent potential fraud.

Claim 16

Shinzaki, in view of Ronning, discloses the limitations of claim 14 as shown above. Furthermore, Ronning, as shown, discloses the following limitation:

- *computer code that communicates to a customer the status of said second online transaction based upon the similarity of said stored customer identification data and the new customer identification data* (see at least column 7, lines 39-42: System 200 determines if the user is attempting a fraudulent transaction and, if not, it downloads the purchased products to the user's machine using a download page 516; also see at least column 9, lines 34-37: If authorization is not obtained (step 503), system 200 declines the order (step 509) and typically presents a message to the user indicating the denial).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). If there is an indication that a transaction is fraudulent, based on the similarity of stored and new customer identification data, then the status of a transaction should be communicated to the customer because he must know whether the transaction will continue (i.e. follow through).

Claim 18

Ronning, as shown, discloses the following limitations:

- *computer code that creates a first computer identifier in the course of an online transaction comprising the steps of Claim 1* (Shinzaki, in view of Ronning, discloses the limitations of claim 1 as shown above);
- *computer code that creates at least one additional computer identifier in the course of an additional online transaction comprising the steps of Claim 1* (Shinzaki, in view of Ronning, discloses the limitations of claim 1 as shown above);
- *computer code that utilizes a matching routine to compare said first computer identifier with said at least one additional computer identifier* (see at least column 9, lines 48-59: The fraud processing involves generating a fraud ranking based upon the user's information in order form 520 and associated information. The associated information may include any information, or a sub-set of that information, having any type of relation to the information submitted with the order. For example, it typically includes information linked with the submitted information as determined by the relational database tables illustrated in FIG. 5C. It may also include a previous fraud ranking or an AVS rating. System 200 may use the submitted information to perform database look ups to obtain associated information for analysis); and
- *computer code that decides as to whether the online transaction is fraudulent, not fraudulent or requires further consideration based on the similarities between said first computer identifier and said at least one additional computer identifier* (see at least column 10, lines 7-10 and 46-49: If the user's fraud ranking passes a particular threshold, indicating a likelihood of an attempted fraudulent transaction, system 200 declines the order (step 509)... System 200 may perform steps 601 604 in any particular order to generate the cumulative fraud ranking, and may perform fewer steps to generate it or perform more steps based upon additional criteria; also see at least column 12, lines 8-11: system 200 compares particular main information on the same order against known profiles indicating attempted fraudulent

transactions (step 712), and it determines if the main information matches the known profiles).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning because of the following reasons: 1) an on-line retailer should safeguard credit card numbers in order to prevent others from obtaining them; 2) an on-line retailer should protect products that are distributed in electronic form to prevent unauthorized access and distribution of the products; and 3) a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 43-51 of Ronning).

Claim 19

Shinzaki, as shown, discloses the following limitations:

- *receiving information relating to an online transaction from a customer's device* (see at least column 3, lines 64-65: receiving data to/from the portable electronic device);
- *capturing a local time from a clock of said customer's device* (see at least column 4, lines 57-58: a time stamp generating section for generating a time stamp as the date and time);
- *capturing a website server's local time from a clock of a website server relating to said online transaction* (see at least column 4, lines 65-66: a clock function section for calculating the current time);
- *calculating a measured delta of time parameter based upon a difference between said customer's device local time and said website server's local time* (see at least column 4, lines 66-67 and column 5, lines 1-3: a time stamp verifying section for comparing the original time stamp… with the current time, which has been calculated by the clock function section).

Shinzaki does not disclose the following limitation, but Ronning, as shown, does:

- *comparing said measured delta of time parameter with a previously determined delta of time parameter associated with said customer's device for discrepancies indicating potential fraud* (see at least column 12, lines 47-67 and column 16, lines 23-30: system 200 retrieves **a piece of information** (delta of time parameter) from the user's submitted order. System 200

> checks a daily bad uses counter by determining the number of times this piece of information appeared on an order that was declined today… System 200 also checks an historical bad uses counter by using a database look up to determine the number of times **this piece of information appeared on an order that was declined historically** (previously determined delta of time parameter)… snapshots may be taken at other points in the process and compared with previous or subsequent snapshots (delta of time parameter). In addition, by using time stamps, system 200 may determine a rate at which information potentially changes within the same order or, for example, a rate at which a user submits a particular piece of information such as a credit card number. The rate information may further be used to detect and prevent fraud).

It would have been obvious to one of ordinary skill in the art at the time of the invention to substitute a delta of time parameter for a piece of information from the user's submitted order because a delta of time parameter is a piece of information that 1) is associated with a user's order much like a time stamp is associated with an order and 2) can help identify the user (see at least Shinzaki column 5, lines 12-15: the user is identified as the authorized user of the portable electronic device, as the comparison result by the biometric feature data verifying section and the time stamp verifying section (delta of time parameter)).

Furthermore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning. Shinzaki discloses receiving information from a customer's device, capturing a computer's local time, capturing a website server's local time, and calculating a delta of time parameter. Shinzaki does not disclose comparing said delta of time parameter with a previously determined delta of time parameter. However, Ronning, discloses comparing a delta of time parameter with a previously determined delta of time parameter. Therefore, it would have been obvious to combine Ronning with Shinzaki because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Comparing a delta of time parameter with a previously determined delta of time parameter is one measure to

help identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

Claim 20

Shinzaki, in view of Ronning, discloses the limitations of claim 19. Furthermore, Ronning discloses the following limitations:

- *said previously determined delta of time parameter was calculated from a previous online transaction between said customer's device and said website server* (see at least column 12, lines 47-67 and column 16, lines 23-30: system 200 retrieves a piece of information from the user's submitted order. System 200 checks a daily bad uses counter by determining the number of times this piece of information appeared on an order that was declined today… System 200 also checks an historical bad uses counter by using a database look up to determine the number of times this piece of information appeared on an order that was declined historically (previously determined delta of time parameter was from a previous online transaction)… snapshots may be taken at other points in the process and compared with previous or subsequent snapshots (previously determined delta of time parameter). In addition, by using time stamps, system 200 may determine a rate at which information potentially changes within the same order or, for example, a rate at which a user submits a particular piece of information such as a credit card number. The rate information may further be used to detect and prevent fraud).

It would have been obvious to one of ordinary skill in the art at the time of the invention to substitute a previously determined delta of time parameter for a piece of information from the database, or a previous snapshot (from a previous transaction), because a previously determined delta of time parameter is a piece of information that 1) is associated with a user's previous order much like a previous time stamp is associated with a previous order and 2) can help identify the user (see at least Shinzaki column 5, lines 12-15: the user is identified as the authorized user of the portable electronic device, as the comparison result by the biometric feature data verifying section and the time stamp verifying section (delta of time parameter)).

Furthermore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning. Shinzaki discloses receiving information from a customer's device, capturing a computer's local time, capturing a website server's local time, and calculating a delta of time parameter. Shinzaki does not disclose using a previously determined delta of time parameter that was calculated from a previous online transaction. However, Ronning, discloses using a previously determined delta of time parameter that was calculated from a previous online transaction. Therefore, it would have been obvious to combine Ronning with Shinzaki because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Using a previously determined delta of time parameter that was calculated from a previous online transaction is one measure to help identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

Claim 21

Shinzaki, in view of Ronning, discloses the limitations of claim 19. Furthermore, Ronning discloses the following limitations:

- *said measured delta of time parameter is compared to said previously determined delta of time parameter to determine whether they are substantially the same* (see at least column 16, lines 23-30: snapshots (measured delta of time parameter) may be taken at other points in the process and compared with **previous or subsequent snapshots**. In addition, **by using time stamps**, system 200 may determine a rate at which information potentially changes (delta of time parameter) within the same order or, for example, a rate at which a user submits a particular piece of information such as a credit card number. The rate information may further be used to detect and prevent fraud (check whether delta of time parameters are the same)).

It would have been obvious to one of ordinary skill in the art at the time of the invention to substitute a delta of time parameter for a snapshot because a delta of time parameter is like a

snapshot in that both 1) are associated with a user's order and 2) can help identify the user (see at least Shinzaki column 5, lines 12-15: the user is identified as the authorized user of the portable electronic device, as the comparison result by the biometric feature data verifying section and the time stamp verifying section (delta of time parameter)). Additionally, Ronning teaches using time stamps to determine changes in an order (comparing delta of time parameters for the order).

Furthermore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning. Shinzaki discloses receiving information from a customer's device, capturing a computer's local time, capturing a website server's local time, and calculating a delta of time parameter. Shinzaki does not disclose comparing a measured delta of time parameter to a previously determined delta of time parameter to determine whether they are the same. However, Ronning, discloses comparing a measured delta of time parameter to a previously determined delta of time parameter to determine whether they are the same. Therefore, it would have been obvious to combine Ronning with Shinzaki because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Comparing a measured delta of time parameter to a previously determined delta of time parameter to determine whether they are the same is one measure to help identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

Claim 22

Shinzaki, in view of Ronning, discloses the limitations of claim 19. Furthermore, Ronning discloses the following limitations:

- *said measured delta of time parameter is substantially constant for said customer's device relative to said previously determined delta of time parameter indicating a low likelihood that said online transaction is fraudulent* (see at least column 16, lines 8-35: If all the snapshots

(delta of time parameters) match (are constant), system 200 proceeds with order processing (low likelihood of fraud)).

It would have been obvious to one of ordinary skill in the art at the time of the invention to substitute a delta of time parameter for a snapshot because a delta of time parameter is like a snapshot in that both 1) are associated with a user's order and 2) can help identify the user (see at least Shinzaki column 5, lines 12-15: the user is identified as the authorized user of the portable electronic device, as the comparison result by the biometric feature data verifying section and the time stamp verifying section (delta of time parameter)). Additionally, Ronning teaches using time stamps to determine changes in an order (comparing delta of time parameters for the order).

Furthermore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning. Shinzaki discloses receiving information from a customer's device, capturing a computer's local time, capturing a website server's local time, and calculating a delta of time parameter. Shinzaki does not disclose having the measured delta of time parameter constant for a device relative to a previously determined delta of time parameter. However, Ronning, discloses having the measured delta of time parameter constant for a device relative to a previously determined delta of time parameter. Therefore, it would have been obvious to combine Ronning with Shinzaki because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Having the measured delta of time parameter constant for a device relative to a previously determined delta of time parameter is one measure to help identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

Claim 23

Shinzaki, in view of Ronning, discloses the limitations of claim 19. Furthermore, Ronning discloses the following limitations:

- *said measured delta of time parameter is compared to said previously determined delta of time parameter to determine whether they fall within a substantially constant range corresponding to said customer's device* (see at least column 16, lines 23-35: snapshots (measured delta of time parameter) may be taken at other points in the process and compared with **previous or subsequent snapshots**. In addition, **by using time stamps**, system 200 may determine a rate at which information potentially changes (delta of time parameter) within the same order or, for example, a rate at which a user submits a particular piece of information such as a credit card number. The rate information may further be used to detect and prevent fraud (check whether delta of time parameters fall within a constant range). For example, system 200 may determine that the same user is repeatedly submitting orders having different credit card numbers in a **short time frame** requesting purchase of the same product, which may indicate attempted fraud).

It would have been obvious to one of ordinary skill in the art at the time of the invention to substitute a delta of time parameter for a snapshot because a delta of time parameter is like a snapshot or time stamp in that both 1) are associated with a user's order and 2) can help identify the user (see at least Shinzaki column 5, lines 12-15: the user is identified as the authorized user of the portable electronic device, as the comparison result by the biometric feature data verifying section and the time stamp verifying section (delta of time parameter)). Additionally, Ronning teaches using time stamps to determine changes in an order (comparing delta of time parameters for the order) and checking the time frame that orders are submitted (fall within a constant range). Furthermore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning. Shinzaki discloses receiving information from a customer's device, capturing a computer's local time, capturing a website server's local time, and calculating a delta of time parameter. Shinzaki does not disclose having the measured delta of time parameter fall within a constant range for a device relative to a previously determined delta of time parameter. However, Ronning, discloses having the measured delta of time parameter fall within a constant range for a

device relative to a previously determined delta of time parameter. Therefore, it would have been obvious to combine Ronning with Shinzaki because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Having the measured delta of time parameter fall within a constant range for a device relative to a previously determined delta of time parameter is one measure to help identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

Claim 24

Shinzaki, in view of Ronning, discloses the limitations of claim 19. Furthermore, Ronning discloses the following limitations:

- *at least one of said measured delta of time parameter and previously determined delta of time parameter is stored by said web server for comparison with a future delta of time parameter measured in the context of a future online transaction to indicate potential fraud* (see at least column 12, lines 47-67: system 200 retrieves **a piece of information** (delta of time parameter) from the user's submitted order. System 200 checks a daily bad uses counter by determining the number of times this piece of information appeared on an order that was declined today (previous delta of time parameter was saved from previous orders to compare against future orders)… System 200 also checks an historical bad uses counter by using a database look up to determine the number of times **this piece of information appeared on an order that was declined historically** (indicate potential fraud).

It would have been obvious to one of ordinary skill in the art at the time of the invention to substitute a delta of time parameter for a piece of information from the user's submitted order because a delta of time parameter is a piece of information that 1) is associated with a user's order much like a time stamp is associated with an order and 2) can help identify the user (see at least Shinzaki column 5, lines 12-15: the user is identified as the authorized user of the portable electronic device, as the comparison result by the biometric feature data verifying section and the time stamp verifying section (delta of time parameter)).

Furthermore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the method of detecting fraud of Ronning. Shinzaki discloses receiving information from a customer's device, capturing a computer's local time, capturing a website server's local time, and calculating a delta of time parameter. Shinzaki does not disclose storing a delta of time parameter for comparison with a future delta of time parameter. However, Ronning, discloses storing a delta of time parameter for comparison with a future delta of time parameter. Therefore, it would have been obvious to combine Ronning with Shinzaki because a need exists for secure electronic commerce to prevent fraudulent attempts (see at least column 1, lines 50-51 of Ronning). Storing a delta of time parameter for comparison with a future delta of time parameter is one measure to help identify the customer and prevent fraud. The more parameters utilized, the more likely the chances of correctly identifying the customer and preventing fraud.

22. Claims 4 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shinzaki, in view of Ronning, and further in view of Boesch et. al. (US 6,092,053).

Claim 4

Shinzaki, in view of Ronning, discloses the limitations of claim 1 as shown above. Furthermore, Boesch, as shown, discloses the following limitation:

- *said at least one non-personal identification parameter is said customer's computer's Browser ID* (see at least column 7, lines 15-19: The message sent from the consumer's browser to the CIS (consumer information server) indicates whether the browser contains a browser identifier. In the preferred embodiment, the browser identifier is a cookie. A browser identifier identifies the consumer browser on a specific consumer computer).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki, in view of Ronning, with the browser ID parameter of Boesch. As shown above, Shinzaki teaches capturing of certain parameters in order to validate a user to prevent fraud. Ronning teaches the need for secure electronic commerce to prevent fraud. Both Shinzaki and Ronning fail to teach capturing a computer's

browser ID to prevent fraud. However, Boesch teaches that capturing a browser ID was a well known parameter in order to detect fraud. Thus, it would have been obvious to combine Shinzaki, in view of Ronning, with Boesch because a browser ID is a parameter that can be used to prevent fraud.

Claim 11

Shinzaki, in view of Ronning, discloses the limitations of claim 6 as shown above. Furthermore, Boesch, as shown, discloses the following limitation:

- *said non-personal identification parameter is a Browser ID* (see at least column 7, lines 15-19: The message sent from the consumer's browser to the CIS (consumer information server) indicates whether the browser contains a browser identifier. In the preferred embodiment, the browser identifier is a cookie. A browser identifier identifies the consumer browser on a specific consumer computer).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki, in view of Ronning, with the browser ID parameter of Boesch. As shown above, Shinzaki teaches capturing of certain parameters in order to validate a user to prevent fraud. Ronning teaches the need for secure electronic commerce to prevent fraud. Both Shinzaki and Ronning fail to teach capturing a computer's browser ID to prevent fraud. However, Boesch teaches that capturing a browser ID was a well known parameter in order to detect fraud. Thus, it would have been obvious to combine Shinzaki, in view of Ronning, with Boesch because a browser ID is a parameter that can be used to prevent fraud.

23. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shinzaki in view of Boesch.

Claim 17

Shinzaki discloses the limitations of claim 12 as shown above. Furthermore, Boesch, as shown, discloses the following limitation:

- *said non-personal computer identification parameter is a Browser ID* (see at least column 7, lines 15-19: The message sent from the consumer's browser to the CIS (consumer information server) indicates whether the browser contains a browser identifier. In the preferred embodiment, the browser identifier is a cookie. A browser identifier identifies the consumer browser on a specific consumer computer).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the user verification functions of Shinzaki with the browser ID parameter of Boesch. As shown above, Shinzaki teaches capturing of certain parameters in order to validate a user to prevent fraud. Shinzaki fails to teach that one of the parameters captured is a computer's browser ID. However, Boesch teaches that capturing a browser ID was a well known parameter in order to detect fraud. Thus, it would have been obvious to combine Shinzaki with Boesch because a browser ID is a parameter that can be used to validate a user to prevent fraud.

Conclusion

Applicant's amendment necessitated the new grounds of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **Chrystina Zelaskiewicz** whose telephone number is **571.270.3940.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **James A. Reagan** can be reached at **571.272.6710**. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair <http://pair-direct.uspto.gov >. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to **571-273-8300**. Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

/Chrystina Zelaskiewicz/Examiner, Art Unit 4143
May 5, 2008
/James A. Reagan/
Supervisory Patent Examiner, Art Unit 4143